UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,024	07/05/2001	Toru Inada	0054-0236P	9286

2292	7590	07/25/2006	

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER
MOORE, IAN N

ART UNIT	PAPER NUMBER
2616	

DATE MAILED: 07/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/898,024	INADA ET AL.
	Examiner	Art Unit	
	Ian N. Moore	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>29 June 2006</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-6</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1,2,4 and 5</u> is/are rejected.

7)☒ Claim(s) <u>3,6</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 1,2, 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Takiyasu et al, hereinafter 'Takiyasu" (US Patent 5,113,392) in view of Bray et al, hereinafter

"Bray" (US005161189A).

With regard to claims 1 and 4, Takiyasu discloses, if the length of a transmission

message is equal to or shorter than 60 bytes (computing the packet length / comparing the

computed packet length with a predetermined packet length), it can be transmitted by using a

single cell. If it is longer than 60 bytes, it can be transmitted after being segmented

(fragmentation unit) into a plurality of information blocks (plurality of divided data groups) on

the 60 byte unit basis (predetermined data structure), which is capable of transmitting (column 6,

lines 17-22). The info field 16 (adding ... control information) indicates the position of a

particular information block. For instance, if the information contained in the info field 16 is the

first information block of a message segmented into multiple blocks, ST 15A is set to "10", "01"

for the last information block, "00" for an intermediate information block and "11" for a single

information block (column 6, lines 22-28), wherein the plurality of information blocks are

transmitted to the transmission destination terminal (see col. 6, line 6-10; see col. 8, line 15-26;

transmission towards destination node).

Takiyasu does not expressly disclose encryption means for separately encrypting the

plurality of divided data packets to form a plurality of encrypted packets; decryption terminal;

two or more associated divided data packets and the control information permits the associated

divided data packets to be decrypted independently without waiting for the arrival of any other

associated divided data packets.

However, Bray teaches encryption means (see FIG. 2, Encryption device 213; or see FIG.

3, encryption device 321,323; see col. 3, line 33-67) for separately encrypting the plurality of

divided data packets to form a plurality of encrypted packets (see FIG. 5A-C; forming a first

second, third, and fourth rekeying message segments 501,503,505,507,509,511,513,515 are

encrypted into a first second, third, and fourth encrypted messages each including a message

header (MH) 519,521,523,525; see col. 1, line 66 to col. 2, line 5; col. 4, line 30-65);

an encrypted packet transmission unit (see FIG. 3, SCSI 313; or see FIG. 2, Transmitter

217) for transmitting the plurality of encrypted packets to a decryption terminal (see FIG. 1,

terminal 107 or KMC 101 with decryption 213,323,321); see col. 3, line 16 to col. 4, line 5;

wherein the plurality of divided two or more associated divided data packets (see FIG.

5C, a first second, third, and fourth rekeying message segments, 503,507,511,515) and the

control information (see FIG. 5C, MH 519,521,523,525) permits the associated divided data

packets to be transmitted to the transmission destination terminal (see FIG. 1, terminal 107 or

KMC 101) independently without waiting for the arrival of any other associated divided data

packets (see FIG. 6, step 601,603,611,613; performing independent decryption on each message

segment; see col. 5, line 43 to col. 6, line 5). Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to provide encryption means

to encrypt message segment and decryption each message segment independently without

waiting for the arrival of other segments, as taught by Bray in the system of Takiyasu, so that it

would save time, energy and necessary RAM storage; see Bray col. 2, line 39-43.

With regard to claims 2 and 5, refer to rejection of claim 1 (cryptographic apparatus).

With specific regards to the additional limitations of claim 2, Takiyasu discloses an

asynchronous port 28 (terminal that receives) that includes a reassemble unit 51 (reconstructs the

divided data groups) (column 8, lines 13-15). The info field 16 (control information) indicates

the position of a particular information block (column 6, lines 22-28). Bray discloses a

decryption apparatus (see FIG. 2, Encryption/decryption device 313; or see FIG. 3, encryption

device 321,323; see col. 3, line 33-67), which receives the plurality of encrypted packets

transmitted from said cryptographic apparatus, separately decrypts each of the plurality of

encrypted packets into the divided data packet (see col. 5, line 43 to col. 6, line 5), and transmits

the plurality of divided data packets in the decryption order (see col. 5, line 52 to col. 6, line 10).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the

invention was made to provide decryption means to encrypt message segment and decryption

each message segment independently without waiting for the arrival of other segments and

transmitting decrypted segments, as taught by Bray in the system of Takiyasu, for the same

motivation as stated above in claims 1 and 4.

Allowable Subject Matter

3.   **Claims 3 and 6** are objected as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

4.   Applicant's arguments with respect to claim 1,2,4, and 5 have been considered but are moot in view of the new ground(s) of rejection.

Regarding claims 1, 2,4,5 and 6, the applicant argued that, "...nowhere in Takiyasu is there any disclosure or suggestion of encrypting packets prior to transmission or of determining the size of the packets after they are encrypted as claimed...nowhere in Takiyasu is there any discussion of encrypting the data packets or the need or desire of encrypting the data packets" in page 10, paragraph 2; page 11, paragraph 3; page 13, paragraph 1,3-4; page 14, paragraph 2-3.

In response to applicant's argument, the examiner respectfully disagrees with the above argument.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., **encrypting packets prior to transmission or of determining the size of the packets after they are encrypted**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the combined system of Takiyasu and Bray discloses all claimed invention. Bray discloses encrypting the data packets or the need or desire of encrypting the data packets as set forth below.

Regarding claims 1,2,4,5 and 6, the applicant argued that, "...nowhere in Bray is there any disclosure or suggestion of separately encrypting a plurality of divided data packets to form a plurality of encrypted packets wherein the plurality of divided data packets include two or more associated divided data packets and control information that permits the associated divided data packets to be independently transmitted to a transmission destination terminal without waiting for the arrival of any other associated divided data packet..." in page 11, paragraph 1; page 13, paragraph 1,3-4; page 14, paragraph 2-3.

In response to applicant's argument, the examiner respectfully disagrees with the above argument.

Bray discloses separately encrypting (**see FIG. 2, Encryption device 213; or see FIG. 3, encryption device 321,323; see col. 3, line 33-67**) the plurality of divided data packets to form a plurality of encrypted packets (**see FIG. 5A-C; forming a first second, third, and fourth rekeying message segments 501,503,505,507,509,511,513,515 are encrypted into a first second, third, and fourth encrypted messages each including a message header (MH) 519,521,523,525; see col. 1, line 66 to col. 2, line 5; col. 4, line 30-65**);

wherein the plurality of divided two or more associated divided data packets (**see FIG.
5C, a first second, third, and fourth rekeying message segments, 503,507,511,515**) and the
control information (**see FIG. 5C, MH 519,521,523,525**) permits the associated divided data
packets to be transmitted to the transmission destination terminal (**see FIG. 1, terminal 107 or
KMC 101**) independently without waiting for the arrival of any other associated divided data
packets (**see FIG. 6, step 601,603,611,613; performing independent decryption on each
message segment; see col. 5, line 43 to col. 6, line 5**).

Regarding claims 1 and 6, the applicant argued that, "...one skilled in the art would
not have been motivated to add encryption...absent proper motivation to combined the teachings
of Takiyasu and Bray..." page 12, paragraph 1-2.

In response to applicant's argument that there is no proper suggestion to combine the
references, the examiner recognizes that obviousness can only be established by combining or
modifying the teachings of the prior art to produce the claimed invention where there is some
teaching, suggestion, or motivation to do so found either in the references themselves or in the
knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071,
5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir.
1992). In this case, it would have been obvious to one having ordinary skill in the art at the time
the invention was made to provide encryption means to encrypt message segment and decryption
each message segment independently without waiting for the arrival of other segments, as taught
by Bray in the system of Takiyasu, so that it would save time, energy and necessary RAM
storage; see Bray col. 2, line 39-43.

Moreover, it is also well known in the art and it would have been obvious to one having

ordinary skill in the art at the time the invention was made by encryption to encrypt message

segment and decryption each message segment independently without waiting for the arrival of

other segments, it would provide data security (by way of encryption and decryption), and

provide efficient transmission since there is no reason to wait for other segments before

encryption/decryption since encryption/decryption are performed separately from

segmentation/assembly process.

Thus, it is clear that the motivations set forth above are proper.

Regarding claims 1,2,4,5 and 6, the applicant argued that, "…neither Takiyasu nor

Bray suggest an cryptographic apparatus the includes a fragmentation determination unit…a

fragmentation unit…ensuring continuity between the divided data packets…Bray cannot be

interpreted as disclosing determining the packet length after encryption…" in page 13, paragraph

1-4; page 14, paragraph 2-3.

In response to applicant's argument, the examiner respectfully disagrees with the

above argument.

The combined system Takiyasu and Bray discloses all argued claimed invention as set

forth in above rejection. In particular, a fragmentation determination unit (means for computing

the packet length / comparing the computed packet length with a predetermined packet length

within a node 200 (FIG. 1) before fragmentation) and a fragmentation unit (see FIG. 5,

segmentation unit 54); column 6, lines 17-22.

In response to applicant's argument that the references fail to show certain features of

applicant's invention, it is noted that the features upon which applicant relies (i.e., **determining**

the packet length after encryption) are not recited in the rejected claim(s). Although the

claims are interpreted in light of the specification, limitations from the specification are not read

into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

5.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

6.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Ian N. Moore whose telephone number is 571-272-3085. The

examiner can normally be reached on 9:00 AM- 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Doris To can be reached on 571-272-7629. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

INM
7-20-06

DORIS H. TO
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600